



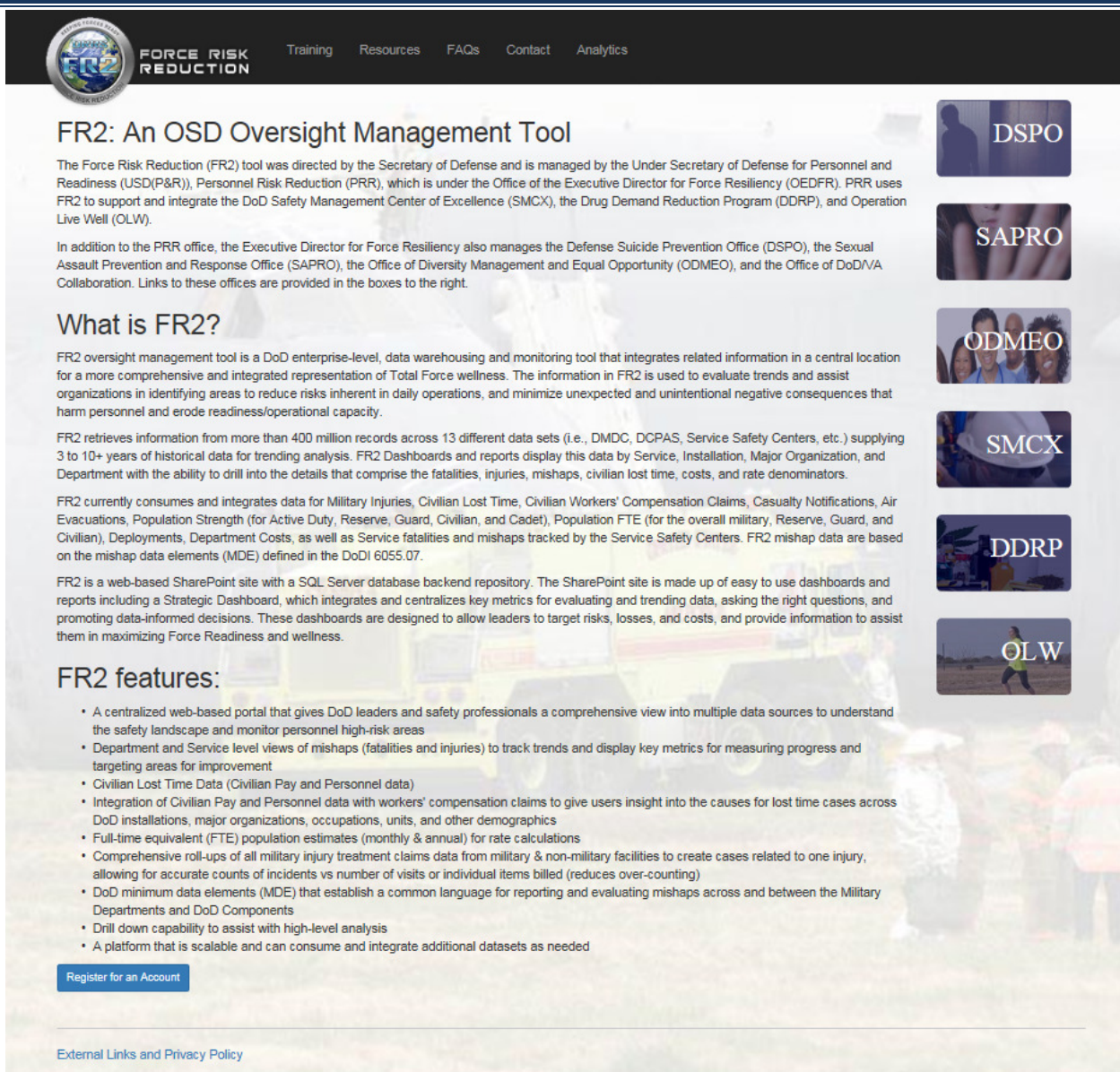
FR2 Quick Reference Sheet

Access to the FR2

Accessing the FR2

The FR2 homepage is located at the URL <https://joint.safety.army.mil/> This is a publicly accessible site, which provides access to the following via links:

- **FR2 Home**
- **Training**
- **Resources**
- **Frequently Asked Questions (FAQs)**
- **Contact**
- **Analytics** – Use this link to access the Analytics Home page that holds the FR2 Dashboards and Reports. This tab is not open access and requires a CAC login.
- **DSPO** – Defense Suicide Prevention Office
- **SAPRO** – Sexual Assault Prevention and Response Office
- **ODMEO** – Office of Diversity Management and Equal Opportunity
- **SMCX** – Safety Management Center of Excellence
- **DDRP** – Drug Demand Reduction Program (DDRP) information page
- **OLW** – Operation Live Well (Health.mil: The official website of the Military Health System and the Defense Health Agency)
- **Register for an Account**
- **External Links and Privacy Policy**



FR2: An OSD Oversight Management Tool

The Force Risk Reduction (FR2) tool was directed by the Secretary of Defense and is managed by the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), Personnel Risk Reduction (PRR), which is under the Office of the Executive Director for Force Resiliency (OEDFR). PRR uses FR2 to support and integrate the DoD Safety Management Center of Excellence (SMCX), the Drug Demand Reduction Program (DDRP), and Operation Live Well (OLW).

In addition to the PRR office, the Executive Director for Force Resiliency also manages the Defense Suicide Prevention Office (DSPO), the Sexual Assault Prevention and Response Office (SAPRO), the Office of Diversity Management and Equal Opportunity (ODMEO), and the Office of DoD/VA Collaboration. Links to these offices are provided in the boxes to the right.

What is FR2?

FR2 oversight management tool is a DoD enterprise-level, data warehousing and monitoring tool that integrates related information in a central location for a more comprehensive and integrated representation of Total Force wellness. The information in FR2 is used to evaluate trends and assist organizations in identifying areas to reduce risks inherent in daily operations, and minimize unexpected and unintentional negative consequences that harm personnel and erode readiness/operational capacity.

FR2 retrieves information from more than 400 million records across 13 different data sets (i.e., DMDC, DCPAS, Service Safety Centers, etc.) supplying 3 to 10+ years of historical data for trending analysis. FR2 Dashboards and reports display this data by Service, Installation, Major Organization, and Department with the ability to drill into the details that comprise the fatalities, injuries, mishaps, civilian lost time, costs, and rate denominators.

FR2 currently consumes and integrates data for Military Injuries, Civilian Lost Time, Civilian Workers' Compensation Claims, Casualty Notifications, Air Evacuations, Population Strength (for Active Duty, Reserve, Guard, Civilian, and Cadet), Population FTE (for the overall military, Reserve, Guard, and Civilian), Deployments, Department Costs, as well as Service fatalities and mishaps tracked by the Service Safety Centers. FR2 mishap data are based on the mishap data elements (MDE) defined in the DoDI 6055.07.

FR2 is a web-based SharePoint site with a SQL Server database backend repository. The SharePoint site is made up of easy to use dashboards and reports including a Strategic Dashboard, which integrates and centralizes key metrics for evaluating and trending data, asking the right questions, and promoting data-informed decisions. These dashboards are designed to allow leaders to target risks, losses, and costs, and provide information to assist them in maximizing Force Readiness and wellness.

FR2 features:

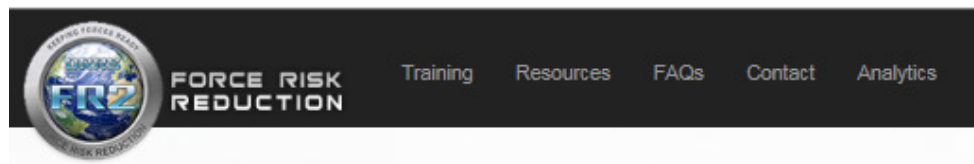
- A centralized web-based portal that gives DoD leaders and safety professionals a comprehensive view into multiple data sources to understand the safety landscape and monitor personnel high-risk areas
- Department and Service level views of mishaps (fatalities and injuries) to track trends and display key metrics for measuring progress and targeting areas for improvement
- Civilian Lost Time Data (Civilian Pay and Personnel data)
- Integration of Civilian Pay and Personnel data with workers' compensation claims to give users insight into the causes for lost time cases across DoD installations, major organizations, occupations, units, and other demographics
- Full-time equivalent (FTE) population estimates (monthly & annual) for rate calculations
- Comprehensive roll-ups of all military injury treatment claims data from military & non-military facilities to create cases related to one injury, allowing for accurate counts of incidents vs number of visits or individual items billed (reduces over-counting)
- DoD minimum data elements (MDE) that establish a common language for reporting and evaluating mishaps across and between the Military Departments and DoD Components
- Drill down capability to assist with high-level analysis
- A platform that is scalable and can consume and integrate additional datasets as needed

[Register for an Account](#)

[External Links and Privacy Policy](#)

Note: The FR2 Web site requires Microsoft Internet Explorer 9 or higher.

Accessing the Analytics Tab



The Analytics homepage that contains FR2 dashboards and reports requires CAC authentication. All users must register for an account:

1. Insert your CAC into the card reader.
2. Click on “Register for an Account” (on the FR2 Home page.)
3. Read the DoD Consent banner at the top and fill out the Account Registration Form.
4. Fill in the required information as requested (you will need to provide your UIC, installation, and major organization). A .mil e-mail address is required for approval.
5. Read the User Agreement and acknowledge it by clicking the checkbox.
6. Acknowledge you have completed Information Assurance training by clicking on the checkbox.
7. Enter your name in the Signature field and select the “Submit Account Registration Request” button.

FORCE RISK REDUCTION Account Registration

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

FR2 Account Registration Form

Please fill out and sign the following form to request access to FR2.

DoDID: 1384621666
DoDID is auto-populated based on your CAC certificate.

Primary UIC:
Start typing your Unit Name or UIC to select from a list of available options.

Installation:
Start typing your Installation Name or ID to select from a list of available options.

Major Organization:
Start typing your Major Organization Name or UIC to select from a list of available options.

Government Affiliation: -- Select a Value --

Parent Organization:

Pay Grade/Rank:

Safety Role:

First Name:

Last Name:

Position:

Commercial Phone:

DSN Phone:

Email:

Reason for Account Request:

Government Sponsor:

Government Sponsor Email:

FORCE RISK REDUCTION (FR2)

USER AGREEMENT

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.
- You consent to the following conditions:
 - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
 - At any time, the U.S. Government may inspect and seize data stored on this information system.
 - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
 - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.
 - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
 - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
 - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception, capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
 - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
 - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
 - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
 - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
 - In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
 - All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

SUPPLEMENTAL PROVISIONS

In addition, you agree to:

- Verify you have received initial Information Assurance (IA) training and will participate in periodic refresher IA awareness training.
- Log in at least every 28 days. If more than 28 days lapse, your account will be disabled, requiring contact with system support.
- Choose strong Passwords that are at least 13 characters in length that include at least one capital letter, one lower case letter, one special character, and one number. Change the Password at least every 90 days.
- Not share Login IDs or account Passwords with anyone, including system administrators.

We reserve the right, in our sole discretion, to terminate your access to all or part of Force Risk Reduction, for any reason, with or without notice. Furthermore, violation of FR2 use policies may result in disciplinary action under applicable administrative, criminal, or contract-based rules, regulations, and state and federal law.

☐ By checking this box, you acknowledge you have read and agree to the FR2 User Agreement.

☐ By checking this box, you acknowledge you have completed Information Assurance (IA) Awareness Training and will take periodic refresher training at <http://iase.diaa.mil/eta/> as required.

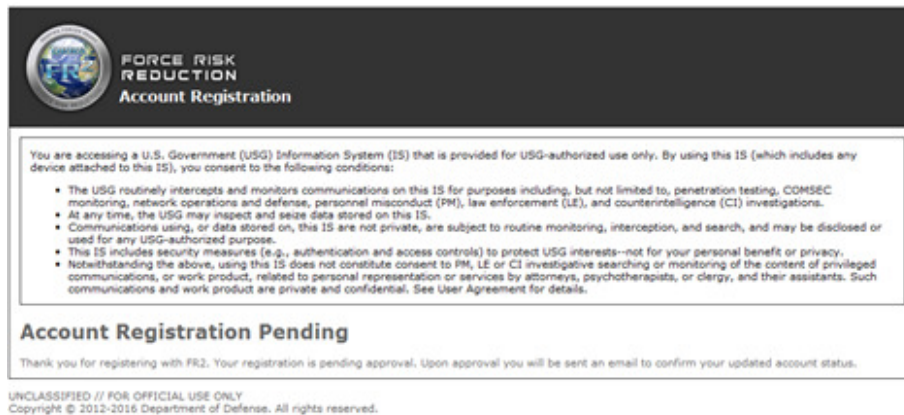
Signature

In adding your name, you agree to abide by the terms of the Force Risk Reduction User Agreement and ongoing Information Assurance training requirements.

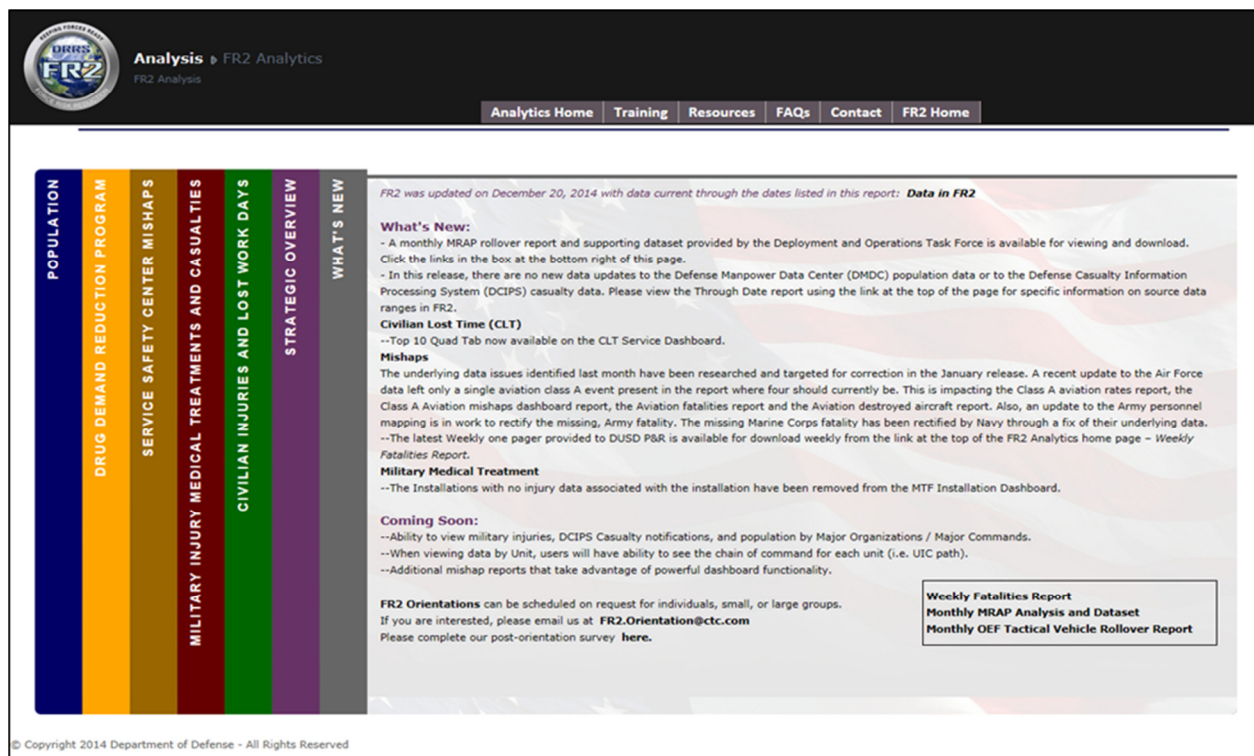
Submit Account Registration Request

Cancel

At this point your screen will change and you will receive an automated email stating that your account request is awaiting approval.



After the FR2 Administrator reviews your account request, you will receive either an approval email or a denial email. Once approved, you will only need to have your CAC inserted into the reader to get into the secured analysis section.



If you have any questions about accessing FR2, contact mailto: fr2.support@camber.com